Submitted by: __Ed Goff, Duke Energy, 919-215-8856 edwin.goff@duke-energy.com_____

Date: _____12-13-13_____

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
							The focus of the Framework should be limited to the systems and assets essential to critical infrastructure functions and this focus should be made clear throughout the Framework and the appendices The scope of risk management is beyond cybersecurity. Organizations must consider a number of business risks (e.g., compliance, financial, operational, and reputational) for business continuity. Risk management is important in understanding and addressing cybersecurity; however, the purpose of the Framework is to "Reduce Cyber Risk to Critical Infrastructure" and not to reduce all broader business risks that an organization might face. Therefore the scope of the Cybersecurity Framework should be clearly limited to cybersecurity for critical infrastructure, the purpose of Executive Order 13636. To "provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach" the Framework's focus must be on the systems and assets essential to critical infrastructure functions. This focus helps ensure that available resources are targeted at reducing critical infrastructure cybersecurity risk. We support the Framework definition of Critical infrastructure in the Introduction and Glossary. However, the scope of the appendices appears to be broader and thereby the focus of the Framework is unclear.	

1	Duke Energy	Ed Goff	G				The Framework Core is particularly confusing as it references “business purposes,” “business needs,” “business objectives,” and other similar business-mission focused language rather than focusing on the systems and assets essential to critical infrastructure functions. Critical infrastructure is not defined by the business missions of each of the 16 sectors identified in PPD-21, but is specific to the operation of the systems and assets critical to the national economy, health, safety, and security. Not all systems and assets within each entity of the 16 critical infrastructure sectors are critical to the nation’s economy, health, safety, and security and therefore not all systems and assets should be the focus of the Framework. The existing, broad business scope will reduce the focus on critical infrastructure and may result in organizations devoting limited resources to systems and assets that are not essential to critical infrastructure functions. As a result, the EO efforts to improve critical infrastructure cybersecurity will be diluted. A risk-based approach focused on the systems and assets essential to the critical infrastructure function enables organizations to identify and prioritize the protection, detection, response, and recovery activities that will help improve critical infrastructure cybersecurity.	The Framework Core is particularly confusing as it references “business purposes,” “business needs,” “business objectives,” and other similar business mission focused language rather than focusing on the systems and assets essential to critical infrastructure functions. Request all instances are have the following appended... "essential for critical infrastructure functions." Detailed recommended changes are included below.

2	Duke Energy	Ed Goff	G			2 & 3	How the Framework Core, Profiles, and Implementation Tiers can be used together to reduce cyber risk to critical infrastructure should be made clear in Section 3.2 The Framework Core (Core) includes the cybersecurity practices that are common across all of the critical infrastructure sectors. This Core provides a baseline set of practices that can be leveraged by organizations to build or improve upon their existing cybersecurity program. The Framework Profile is intended to be "a tool to enable organizations to establish a roadmap for reducing cybersecurity risk." However, the Framework is unclear regarding how the profiles are built using the Core; the Implementation Tiers focus on the maturity of an organization's risk management process rather than implementation of the Core practices. A risk-based approach requires a cybersecurity risk assessment to prioritize these risks, which can be addressed through specific cybersecurity practices. Risk assessment and prioritization is addressed under the Identify function of the Core and the other Core functions address best practices that can be used to respond to cybersecurity risk.	A possible approach to clarifying the use of the Core, Profiles, and Implementation Tiers is: • Step 1: Integrate cybersecurity into an existing or new risk management process to address the applicable categories and subcategories of the Identify Function • Step 2: Based on the risk assessment and prioritization created by the implementation of a risk management process (Step 1), implement the applicable practices found in the categories and subcategories of the Core functions Protect, Detect, Respond, and Recover. During this implementation step, profiles can be created to establish a roadmap and track progress toward reducing cybersecurity risk. • Step 3 (ongoing): Once integrated, the risk management process can be periodically reviewed against the Implementation Tiers to mature the process. This is an ongoing process that will require assessing risk, reprioritizing, and making changes to the applicable cybersecurity practices found in the Core. If this approach is not used, there are specific edits to the existing steps below items 36-42.

3	Duke Energy	Ed Goff	G			App A	The subcategory language should be edited to reduce redundancy, focus on clear outcomes, and relate to the risk management process We greatly appreciate NIST's recent efforts toward improving the subcategory language in the Framework Core. Non-prescriptive language at the cross-sector level is appropriate because diverse users can select the appropriate controls and technologies to meet the cybersecurity outcomes described in the Core. However, in some areas of the core, the subcategory language is redundant and vague, which may lead to inconsistent interpretations within and across the 16 critical infrastructure sectors. Regarding redundancy and vagueness, many of these details will be addressed by individual entities providing comments using the NIST template. As a vagueness example, several subcategories use "managed," "protected," or "secured." It is unclear what these terms mean and how they differ from each other. Each subcategory should be managed under the risk management process, but determining whether an asset is protected or secured is uncertain as the organizations' risk environments vary and change over time. Therefore relating these terms in the subcategory language to the risk management process will add the needed clarity.	Detailed recommendations are included below to address these specific concerns.

4	Duke Energy	Ed Goff	G			3	Section 3.0 of the Framework should support sector-level coordination to develop implementation guidance Efforts to improve cybersecurity are not new to the Energy Sector. The Sector already uses a number of sector specific standards, guidelines, and practices, which can be aligned with the Framework. Examples include the North American Electric Reliability Critical Infrastructure Protection Standards (NERC CIP Standards), the Electricity Subsector Cybersecurity Capabilities and Maturity Model (ES–C2M2), and the Electricity Subsector Cybersecurity Risk Management Process (RMP). As a result, DOE, DHS, NERC, trade organizations, and asset owners and operators of the Energy Sector, have already devoted significant resources towards reducing cyber risk. To encourage critical infrastructure owner and operator use of the Framework, we recommend that NIST support the sector-level effort as described by Section 8 (b) of the Executive Order in the Framework's Section 3.0, How to Use the Framework. In Section 3.0, NIST should encourage the sectors to coordinate with their Sector-Specific Agencies, through their Sector Coordinating Councils to review the Cybersecurity Framework and develop implementation guidance to integrate existing and future efforts "to address sector-specific risks and operating environments." This will enable the Energy Sector to leverage and integrate cybersecurity improvements already underway into the Framework. Also, at the sector-level, cybersecurity risk management can be tailored to unique sector characteristics and leverage expertise from across the sector to increase efficiency and properly leverage asset owner and operator resources to use the Framework to reduce	

5	Duke Energy	Ed Goff	G				The body of the Framework should make it clear that the use or applicability of the subcategories may vary by organization Although the introductory text in Appendix A, the Core, mentions that the Core is not exhaustive and is extensible, this direction is not found in the body of the Framework. The use of subcategories will vary by organizations within and across the 16 critical infrastructure sectors depending on their particular critical infrastructure systems, assets, and risk. For example, the Energy Sector not only includes organizations of various size and ownership structures, but also organizations that are a part of other critical infrastructures. Establishing new protective cybersecurity technological or procedural controls can also undermine existing protections if not executed in a thoughtful, coordinated manner. Not all subcategories, therefore, may be applicable and some categories may need to be added during implementation to address a specific risk to a particular sector or organization. Therefore it should be made clear in the body of the Framework (including Sections 1.1, 2.0, and 3.0) that the use or applicability of the subcategories may vary by organization. This will help to encourage organizations to make well-reasoned, risk-based cybersecurity decisions.	

6	Duke Energy	Ed Goff	G				The definition of Framework adoption has not obtained general consensus In the December 4, 2013 “Update on the Development of the Cybersecurity Framework” (Update), NIST described that “general consensus” was developed based on discussion at the November Raleigh Workshop for a definition of Framework adoption. However, we did not observe such a consensus, but we did observe that the Workshop audience did not generally accept the term or clearly understand the definition of adoption. The definition provided by NIST in the Update was proposed by DHS for discussion specific to the Voluntary Critical Infrastructure Cybersecurity Program (Program), but has not yet received general consensus. We recommend that NIST simplify the adoption definition to: an organization adopts the framework when it voluntarily uses the framework as a part of its risk management process or strategy to protect critical infrastructure.	
7	Duke Energy	Ed Goff	E	2	116	1.1	"best practices" are generally regarded as aspirational and above what is necessary for adequate protection	REMOVE "and best practices"
8	Duke Energy	Ed Goff	T	2	117	1.1	It is unnecessary to require "senior executive level"	Change "senior executive level" to "management"
9	Duke Energy	Ed Goff	E	2	119	1.1	In it's current form, the Framework is not "strategic"	remove ", strategic"
10	Duke Energy	Ed Goff	E	2	123	1.1	In it's current form, the Framework is not "strategic"	remove ", strategic"
11	Duke Energy	Ed Goff	T	3	147	1.1	"other business needs" is broader scope than directed in EO 13636	change "other business needs" to "other critical infrastructure needs"
12	Duke Energy	Ed Goff	T	3	153	1.1	"business/mission objectives" is broader scope than directed in EO 13636	change ""business/mission objectives" to "critical infrastructure objectives"
13	Duke Energy	Ed Goff	T	5	207	2.1	missing word	add "example" between "and Informative"

14	Duke Energy	Ed Goff	T	5	210	2.1	"commonly used" may be inaccurate for many organizations	change "commonly used" to "example"
15	Duke Energy	Ed Goff	T	5	211	2.1	missing word	add "example" between "and Informative"
16	Duke Energy	Ed Goff	T	6	223	2.1	"delivery of services" is too broad	change "delivery of services" to "critical infrastructure functions" or "critical infrastructure services"
17	Duke Energy	Ed Goff	T	6	232	2.1	missing word	add "example" in front of "Informative"
18	Duke Energy	Ed Goff	T	6	242	2.1	"both IT and ICS" may confuse our directed scope	change "both IT and ICS" to "critical infrastructure functions" or "critical infrastructure services"
19	Duke Energy	Ed Goff	T	6	251	2.1	"with the business needs or the organization" is confusing way to end the sentence.	change "with the business needs or the organization" to supporting essential critical infrastructure functions"
20	Duke Energy	Ed Goff	T	7	259	2.1	missing words	add to the end of the sentence "that may impact critical infrastructure functions" or "that may impact critical infrastructure services"
21	Duke Energy	Ed Goff	T	7	264	2.1	missing words	add to the end of the sentence "to critical infrastructure functions" or "to critical infrastructure services"
22	Duke Energy	Ed Goff	T	7	267	2.1	missing words	add to the end of the sentence "involving critical infrastructure functions" or "involving critical infrastructure services"
23	Duke Energy	Ed Goff	T	7	274	2.1	missing words	change "restore the capabilities" to "restore critical infrastructure capabilities"
24	Duke Energy	Ed Goff	T	7	280	2.1	missing words	change "reduce the impact to" to "reduce impact to critical infrastructure functions" or "reduce impact to critical infrastructure services"
25	Duke Energy	Ed Goff	T	7	290-291	2.2	"business/mission requirements" is broader scope than directed in EO 13636	change ""business/mission requirements" to "critical infrastructure"
26	Duke Energy	Ed Goff	E	7	293	2.2	"best practices" are generally regarded as aspirational and above what is necessary for adequate protection	REMOVE "and best practices"
27	Duke Energy	Ed Goff	T	8	310	2.3	missing words	Insert "relative to critical infrastructure" between "priorities, available"
28	Duke Energy	Ed Goff	T	8	316	2.3	prescribing senior executive level is not necessary	Change "senior executive level" to "management"
29	Duke Energy	Ed Goff	T	9	328	2.4	"desired" is unclear and subjective	replace "desired" with "needed"
30	Duke Energy	Ed Goff	T	9	337	2.4	"business/mission requirements" is broader scope than directed in EO 13636	change ""business/mission requirements" to "capabilities and functions essential to critical infrastructure"

31	Duke Energy	Ed Goff	T	10	348	2.4	"approved" by management implies an artifact that demonstrates formal approval	change "approved" to "supported"
32	Duke Energy	Ed Goff	T	10	352	2.4	"management approved" by management implies an artifact that demonstrates formal approval	remove "management approved"
33	Duke Energy	Ed Goff	T	10	356	2.4	"in the larger ecosystem" is vague and unclear	change "in the larger ecosystem" to "sector and with other dependant critical infrastructures"
34	Duke Energy	Ed Goff	T	10	379	2.4	missing words	add "that may impact critical infrastructure functions or services" to the end of the sentence that ends with "address potential cybersecurity events"
35	Duke Energy	Ed Goff	T	10	382	2.4	missing words	add to the end of the sentence "that support critical infrastructure functions" or "that support critical infrastructure services"
36	Duke Energy	Ed Goff	T	11	409	3.2	the purpose of the program is for improved cybersecurity critical infrastructure	change the title of the section to " Establishing or Improving Critical Infrastructure Cybersecurity"
37	Duke Energy	Ed Goff	E	11	410	3.2	un-needed word	remove "recursive"
38	Duke Energy	Ed Goff	T	11	411	3.2	the purpose of the program is for improved cybersecurity critical infrastructure	replace the last part of the sentence beginning with "create…" with protect critical infrastructure."
39	Duke Energy	Ed Goff	T	11	412	3.2	wrong word	replace "mission" with "critical infrastructure"
40	Duke Energy	Ed Goff	T	12	419	3.2	wrong words	replace "on the organization" with "on critical infrastructure functions." or "on critical infrastructure services."
41	Duke Energy	Ed Goff	T	12	424	3.2	"desired" is unclear and subjective	replace "desired" with "required"
42	Duke Energy	Ed Goff	T	12	434	3.2	missing word	insert "example" between "identifies" and "Informative"
43	Duke Energy	Ed Goff	T	13		App A	IDENTIFY FUNCTION - Asset Management Category is missing words	add "functions essential to critical infrastructure" between "objectives" and "and"
44	Duke Energy	Ed Goff	T	13		ID-AM-3	Scope concern - ID-AM-3 is worded as if all communications and data flows are mapped.	add words that scope this to "critical" between "organization" and "communications" or append "for important for critical functions" to the end of the sentence
45	Duke Energy	Ed Goff	T	14		ID-AM-4	Scope concern - ID-AM-4 is worded as if all systems are mapped and catalogued	add words that scope this to "critical" between "organization" and "communications" or append "for important for critical functions" to the end of the sentence
46	Duke Energy	Ed Goff	T	14		ID-AM-5	missing words to clarify subcategory scope	change "business value" to "importance to critical infrastructure"

47	Duke Energy	Ed Goff	T	14		ID-IM-6	missing words to clarify subcategory scope	change "business functions" to "critical infrastructure functions"
48	Duke Energy	Ed Goff	T	14		App A	IDENTIFY FUNCTION - Business Environment Category is missing words	add "critical infrastructure functions" in front of "mission objectives"
49	Duke Energy	Ed Goff	T	14		ID-BE-3	missing words to clarify subcategory scope	change "organizational mission" to "critical infrastructure mission" or add "critical infrastructure" in front of "organization"
50	Duke Energy	Ed Goff	T	14		ID-BE-4	this is an example of a correctly scoped subcategory	please duplicate this approach to other subcategories
51	Duke Energy	Ed Goff	T	15		ID-BE-5	this is an example of a correctly scoped subcategory. Also, the emphasis on "resilience" is more what we expected in the CSF.	please duplicate this approach to other subcategories
52	Duke Energy	Ed Goff	T	15		ID-RA-1	scope concern - ID-RA-1 is worded as if all vulnerabilities are documented	add words that scope this to "critical" or "important for critical functions"
53	Duke Energy	Ed Goff	T	16		ID-RM-3	this is an example of a correctly scoped subcategory.	please duplicate this approach to other subcategories
54	Duke Energy	Ed Goff	T	19		PR-DS-5	subcategory is redundant PR-DS-1 & 2 already require data protection. Specifying "leak" protections seems to get in to the "how" versus the "what"	remove PR-DS-5
55	Duke Energy	Ed Goff	T	19		PR-DS-9	subcategory is redundant PR-DS-1 & 2 already require data protection. Also, with the differences in definitions of PII in the different states we operate in make the use of PII problematic. Clearly, protection of all instances of PII is paramount.	remove PR-DS-9
56	Duke Energy	Ed Goff	T	21		PR-PR-10	scope concern - PR-PR-10 is worded as if all response plans are exercised. This doesn't scale.	add "supporting critical infrastructure functions" in after "plans"
57	Duke Energy	Ed Goff	T	21		PR-PT-3	subcategory is redundant with the Access Control Category	remove PR-PT-3
58	Duke Energy	Ed Goff	T	22		DE-AE-3	scope issue - subcategory is worded as if all "cybersecurity data" is correlated. This doesn't scale.	change "data" to "events" also, this needs to be tied to critical infrastructure assets or functions.
59	Duke Energy	Ed Goff	T	23		DE-DP-1	redundant with ID-DV-2	
60	Duke Energy	Ed Goff	T	23		DE-DP-3	redundant with ID-DV-3	
61	Duke Energy	Ed Goff	T	23		DE-DP-5	redundant with PR-IP-7	

62	Duke Energy	Ed Goff	T	24		RS-AN-1	scope issue - subcategory is worded as if all "notifications" are investigated. This doesn't scale.	add words that scope this to "critical" or "important for critical functions". Otherwise, "high risk" may work here.
63	Duke Energy	Ed Goff	T	36	497	App C	Unclear how these areas became high priority, suggest that they are more potential areas for improvement that have been listed and described.	delete "high-priority," replace with "potential"
64	Duke Energy	Ed Goff	T	36	498	App C	How these were "identified" is unclear, suggest edits to be consistent with these areas are a discussion starting point, more work needs to be done.	replace "currently identified" with "listed and discussed below."
65	Duke Energy	Ed Goff	E	36	498	App C		change "These initial" to "The following"
66	Duke Energy	Ed Goff	T	36	498	App C	A list and description is not really a roadmap, but a starting point for discussion.	change "roadmap" to "discussion starting point"
67	Duke Energy	Ed Goff	T	36	509-516	App C	This discussion is premature, the existing framework needs to be tested first, then a more informed process to develop areas for improvement should come out of the Sector-Specific Agencies through the Sector Coordinating Councils	delete "but these highlighted…addressing the challenges."
68	Duke Energy	Ed Goff	T	36	518-522	App C	Prescriptive discussion, should be sector-specific and not in the NIST Framework.	delete "As a result, …such as a biometric."
69	Duke Energy	Ed Goff	T	38	576-584	App C	This is not an exhaustive list, sector-specific efforts are underway that are not included here, which can be confusing to the reader, lines 568-574 are adequate to address the area.	delete lines 576-584
70	Duke Energy	Ed Goff	G	37	537	App C	Automated Indicator Sharing – Automation is goodness; however, manual sharing (e.g. email, portal, real time conference calls) are useful while we build out automation.	add language to mature manual sharing as an interim improvement opportunity.
71	Duke Energy	Ed Goff	T	38-39	616-617	App C	Appendix B's scope is too large, should be focused on critical infrastructure cybersecurity activities.	delete "including the Privacy Methodology in Appendix B."

72	Duke Energy	Ed Goff	T	39	617-626	App C	A detailed description of the shortcomings of the FIPPs is not needed here, get to the gap.	delete "Although the FIPPs…Privacy Methodology is limited." add "However, the FIPPs do not provide best practices and metrics for implementing privacy protections." delete "lack of standardization, and supporting privacy metrics,"
73	Duke Energy	Ed Goff	G	42	686-741	App E	We should not include terms with existing definitions for many reasons. We should use (reference) existing standards as directed by the EO. Also, there was a request in the last workshop to expand the list of defined terms. We disagree and would like to leverage existing standards and definitions that have already been vetted and published.	Add specific references where definitions were sourced (like ES-C2M2 does) and/or REMOVE definitions for: PII, risk, & risk management.

74	Duke Energy	Ed Goff	G			App B	Appendix B should be revised to focus on protecting privacy and civil liberties implicated by critical infrastructure cybersecurity activities Section 7(c) of the Executive Order specifies that "[t]he Cybersecurity Framework shall include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and individual liberties." Protecting the customer privacy and civil liberties is important. However, we are concerned that, instead of focusing on means to limit the privacy impacts of the Framework, Appendix B appears to recommend independent privacy protections unrelated to the protection of critical infrastructure. Similar to risk management, the scope of privacy and civil liberty protections are beyond that of cybersecurity. The purpose of the framework is to “help owners and operators of critical infrastructure identify, assess, and manage cyber risk.” The methodology in Appendix B should be revised to tailor the methodology to the purpose of the Framework: to improve critical infrastructure cybersecurity. Additionally, it is critical that the privacy methodology is clear and actionable. The existing Appendix B does not readily allow	